09-51

Questions posed by: Jennifer A. Manner
(Sept. 11 letter) Deputy Chief
Public Safety and Homeland Security Bureau
jennifer.manner@fcc.gov

Response from : Pete Eggimann
Director of 911 Services
Metropolitan Emergency Services Board
St. Paul, MN
651 643 8377
peggimann@mn-mesb.org

September 30, 2009

Questions

- What public safety applications must be offered as mission critical standards of quality and does that include broadband communications? In an emergency what can be considered lower priority, voice or data?

  Broadband public safety networks will be used for mission critical applications such as NG9-1-1. This means the networks must be built to mission critical standards, even though not every application on the network is mission critical.

  The public safety broadband network that we believe is necessary in the Minneapolis / St. Paul metropolitan area needs to be as reliable as our current 9-1-1 system is. We don't want to lose reliability as we transition from analog systems to IP-based systems. Since the broadband network will support multiple public safety applications, the network cannot contain any single point of failure. We believe we can obtain a "five 9's" reliable network by using diversity in network paths and redundancy in network components, similar to the way the telephone companies design and implement their SS7 networks.

  In response to the second part of your question regarding prioritization, I would agree that the broadband network will need mechanisms to prioritize the IP traffic from the various applications sharing the network. I think characterization of the IP packets in terms of voice or data may be confusing. All of the packets moving across the broadband network will contain "data". To be understandable and to accurately transmit background noise, a 9-1-1 call carried on a broadband network will need sufficient bandwidth, or priority, to ensure the data packets can be transmitted and received without jitter or latency. Radio voice traffic data packets also need sufficient bandwidth to minimize jitter and latency. Video and image data packets can be buffered and then displayed allowing a lower bandwidth access priority, even though those media formats typically need more total bandwidth than voice applications. Text data packet traffic that is meant to be read by someone on the system can be useable even when there is some latency in the data delivery. Text or numerical data that is meant to control some automated function on the system may require a higher priority. In a nationwide broadband network some prioritization may be possible at the national level, but some level of prioritization control should be available at the regional level in order to accommodate the local variations in the way the network is used.

- Besides video, which public safety application has the highest required data rate, and what is it? Which has the highest sustained bandwidth requirement?

  I think you can make some general assumptions at this point about how a public safety broadband network would be used, but we won't know for sure until we have some actual experience. As I mentioned in my answer to your first question, any kind of high resolution image will require significant bandwidth. This could include building blue prints, aerial photography, or even fingerprints.

  I believe we will also do more bridging of communications from multiple response agencies and incident command structures. Bridged communications tend to tie up significant amounts of bandwidth. In a dedicated public safety broadband network I think it would be prudent to design the network to support day to day operations using no more than 40% of the network capacity, with no single link or component in the network carrying more than 40% of the daily load. This kind of loading will give you the bandwidth necessary to handle high profile events. It also allows you to take down any particular link or component in your network for routine maintenance or replacement without affecting day to day operations. A combination of dedicated bandwidth and prioritization may provide the same level of reliability in a shared commercial / public safety network.

- During an emergency involving multiple public safety agencies operating over the same shared network, who should be in charge of determining which users or which traffic are allowed on the system and which have priority access?

  I believe that a nationwide public safety broadband network should be made up of interconnected state and regional broadband networks. This configuration would require management organizations at the regional (e.g. a public safety joint powers organization representing several counties), the state, and at the national level.

  The regional priorities need to be established cooperatively by the entity responsible for managing the network in that particular region and the emergency communications and response agencies in that region. Consideration needs to be given to prioritization during day to day operations, as well as pre-planning for a major emergency event involving several response agencies. Should the automated system prioritization plan fail during a major event, there needs to be a real time capability to modify the regional prioritization plan (e.g. shift video and image transmission to the Internet to free up bandwidth for voice applications on the regional portion of the dedicated public safety broadband network.)

- How can Federal grant programs encourage equitable distribution of funding to create a more reliable national network for public safety, while making broadband deployment less complicated at the local level? Are there near and long term priorities that grants should target?

  Grant programs should require state level implementation plans with on-going operational / maintenance funding identified. These plans should address all aspects of public safety response including military, EMS, fire, law enforcement, and emergency communications. Consideration should also be given to involving the medical service providers, public utilities, and transportation departments, particularly as to how those entities would be utilized in a major catastrophe response.

Grant programs should require a plan in which the grant applicants demonstrate that they are planning for the future and that investments are designed to take advantage of modem IP-based, broadband-enabled technologies. Recognizing that IP and broadband enable a fundamentally new environment in which multiple public safety agencies and functions can share networks, databases, services, and applications, grant applicants should be required to demonstrate how grant funds are being utilized to the benefit of as many agencies and functions as possible to create system efficiencies and economies of scale. For example, grant reviewers should question separate grant applications in the same region that are separately applying for funds for unique IP backbone networks for 9-1-1 and law enforcement information sharing. In that example applicants should be required to demonstrate why two stand-alone networks are justified. Also, assuming this model is adopted and multiple entities are sharing networks, databases, services, and applications, grant programs must ensure that the applicants have an effective governance structure in place, or plans to establish an appropriate structure, to address complex issues (many of which are raised in the questions above).

Finally, in addition to grants, federal and state governments should be encouraged to look at more long-term and annually recurring funding sources for 9-1-1 and public safety broadband needs. While grant programs are good, funding in the form of a one-time appropriation alone is insufficient. Relying on a onetime, or even *potentially* repeated annual appropriations for grants, does not allow states, localities and industry to effectively plan for the future with any confidence or predictability that funds for public safety broadband services and applications will be available. The FCC, Congress and others should also consider potential funding alternatives in addition to grants, including methods that could raise funds monthly to be deposited into a public safety broadband trust fund, for example. Such methods could include, but are not limited to, (1) establishing an E-Rate-like program similar to the method in which schools and libraries have access to an annual fund for Internet connections, (2) providing the FCC with authority to impose a monthly broadband fee on all telecommunication customers collected by service providers for the express purpose of public safety broadband service, or (3) imposing a fee at the point of sale of communication devices capable of dialing or reaching 9-1-1 centers. These types of funding sources may be a challenge to implement, but it is important that we work together to identify known and recurring sources of funding for public safety's broadband needs.

- Do you envision a time when broadband communications will supplant legacy LMR emergency communications systems? What would need to happen in order for such an outcome to be achieved?

  I think it is clear that converged, broadband-based communications will replace all of the legacy communications systems that we think of today, such as telephone systems and LMR. Smart phone-type devices capable of receiving voice, text, and multimedia communication formats will replace the law enforcement officer or paramedic's portable radio. Emergency vehicles will contain similar multimedia communication devices, and may also become mobile hotspots to support the individual responder personal devices. All of these devices will be able to operate on multiple broadband networks. These systems need to support "presence" (agency and user identification) and automatic location determination for the devices that are active.

This type of converged communications system will be based on open standards that support interoperability between networks and the applications running on those networks. This level of interoperability involves all applications, not just radio communications. If this converged network is a shared commercial / public safety network, the ability to give public safety users priority over the general public would be critical to allow support for mission critical applications.

- What is the current thinking on solutions to the geo-location problem in NG911? What do they think is the problem?

  I think the biggest problem that has not been adequately addressed yet involves the need for the last mile access networks to automatically provide the location of devices on the network when the device is used to make a 9-1-1 call. I believe that almost all new personal communications devices or services will be either nomadic or mobile with the capability to utilize multiple access networks, wired and wireless.

  9-1-1 system support of this type of device or service, will require all Internet or telecommunications service providers (cable, telephone, satellite, WiFi, WiMAX, wireless telephone, etc.) to map their networks and locate a device in real time. The device location, or a query key used to retrieve the location, inserted into the 9-1-1 call setup information, would be used to route the call. The location would arrive at the 9-1-1 center with the call, or could be retrieved by the 9-1-1 center equipment. Getting service providers to provide this location information will involve some level of regulation or financial incentive. The service providers will also need to follow the same interoperability standards that public safety uses so that the location information can be passed between systems and applications.

Federal Communications Commission
Washington, D.C. 20554

September 11, 2009

Mr. Pete Eggimann
Director
Metropolitan Emergency Services Board
2099 University Avenue, West
St. Paul, MN 55104
peggimann@mn-mesb.org

Dear Mr. Eggimann:

Thank you very much for your participation in the FCC's August 25th Public Safety and Homeland Security Workshop. This Workshop had the highest attendance of any workshop to date, which demonstrates how important these issues are to the Broadband Plan and the American people, including the public safety community.

As you know, we were on a very tight schedule and therefore could not get to each question posed to the panel from both our in-house and online audience. If you could take a few moments to answer the following questions and provide us your answers by October 1st, 2009 we would appreciate it. Of course, your answers will be made part of the public record for the Broadband Plan Proceeding.

Questions

What public safety applications must be offered as mission critical standards of quality and does that include broadband communications? In an emergency what can be considered lower priority, voice or data?

- Besides video, which public safety application has the highest required data rate, and what is it? Which has the highest sustained bandwidth requirement?

- During an emergency involving multiple public safety agencies operating over the same shared network, who should be in charge of determining which users or which traffic are allowed on the system and which have priority access?

- How can Federal grant programs encourage equitable distribution of funding to create a more reliable national network for public safety, while making broadband deployment less complicated at the local level? Are there near and long term priorities that grants should target?

- Do you envision a time when broadband communications will supplant legacy LMR emergency communications systems? What would need to happen in order for such an outcome to be achieved?

- What is the current thinking on solutions to the geo-location problem in NG911?

Thank you once again. Your contribution will help us shape a bold and innovative vision for how broadband can serve our country's public safety community. If you have any questions or comments please feel free to contact me at (202) 418-3619 at your convenience.

Sincerely,

Jennifer A. Manner
Deputy Chief
Public Safety and Homeland Security Bureau
Jennifer.Manner@fcc.gov